REMARKS

Applicants appreciate the thorough examination of the present application that is reflected in the Final Official Action. Applicants have studied the Examiner's newly introduced basis of rejecting the independent claims based on England, and respectfully submit that the pending claims are patentable over England, Bjorn, and Matchett for the reasons that now will be described.

The Web Addresses Have Been Amended

The specification has been objected to on page 2, section 2, of the Final Office Action on the basis that disclosed web addresses are executable. In accordance with the Examiner's suggestion for overcoming this objection, the specification has been amended to place the references to web addresses within quotation marks. Accordingly, Applicants respectfully submit that the objections relating thereto have been overcome.

Independent Claims 26, 27, 60, 61, 94, 95, and 103-105 Are Patentable Over Bjorn in view of Matchett, and further in view of England.

Independent Claims 26, 27, 60, 61, 94, 95, and 103-105 stand formally rejected as unpatentable over Bjorn in view of Matchett. Applicants explained in detail in their Amendment filed October 26, 2004 why the pending claims are patentable over Bjorn in view of Matchett. The Final Office Action appears to concede that Bjorn and Matchett do not teach all of the recitations of these claims by its citation for the first time to England. In particular, on Pages 2-2, Section 2.1, of the Final Office Action, the Examiner states the following:

> Applicant has amended the independent claims by combining some of the dependent claims to recite for example the step of "concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remain connected until completion of the security-sensitive operation." This added limitation can be found in one of the cited art (England, column 11, line 54 through column 12, line 8).

Initially, Applicants note that the Examiner has not made a formal rejection of any of the claims in view of England. However, even if the pending claims are rejected in view of England, the cited portion of England recites the following:

> The operating system checks the signature of a component before loading it (block 303). If the signature is valid (block 305), the component has not been compromised by someone attempting to circumvent the boot process and the process proceeds to check the level of trust assigned to the component (block 307). If the signature is not valid (or if there is no signature) but the component must be loaded (block 319), the operating system will not assume the identity of a DRMOS upon completion of the boot process as explained further below.
>
> A plug-and-play operating system provides an environment in which devices and their supporting software components can be added to the computer during normal operation rather than requiring all components be loaded during the boot process. If the device requires the loading of an untrusted component after the boot process completes, a plug-and-play DRMOS must then "renounce" its trusted identity and terminate any executing trusted applications (block 323) before loading the component. The determination that an untrusted component must be loaded can be based on a system configuration parameter or on instructions from the user of the computer.

((England, column 11, line 54 through column 12, line 8, emphasis added).

The cited portion of England is a description of FIG. 3 of that reference which is shown below on the following page.

FIG. 3 of ENGLAND

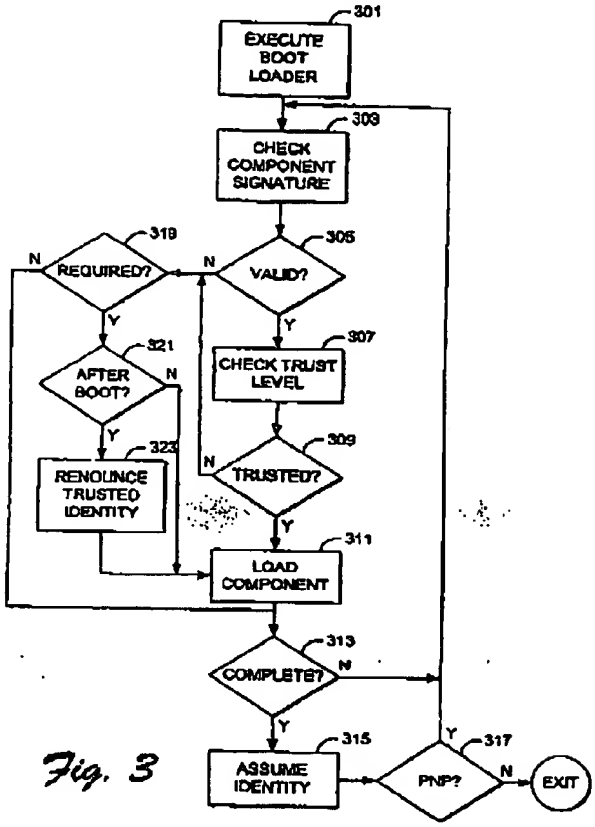


Fig. 3

Referring to FIG. 3, England describes that a component can be verified and loaded during or after a boot process. Referring to Block 303, England describes that an "operating system [that] checks the signature of a component before loading it" to determine whether it is trusted or untrusted. (England, column 11, lines 54-55). England also describes that "all components are signed by a trusted source and provided with a rights manager certificate", the rights manager certificate is the signature that is checked by the operating system. (England, column 11, lines 50-51). When the signature is determined to be valid (at Blocks 305-307), the component is loaded at Block 311 into the operating system irrespective of whether the component is being loaded during the boot process or after the boot process. It is only when the signature from a component is determined at Block 305 to be invalid does the operating system perform a further check at Block 321 as to whether the component is being tested after the boot process and, if so, then at Block 323 the operating system renounces its trust of the component and then loads the component at Block 311.

Applicants submit that nowhere does England disclose that the operating system determines whether a component is trusted or untrusted based on whether the component has remained connected to the computer. Instead, the operating system of England tests only the signature (rights manager certificate) received from the component to determine whether it is to be trusted. Consequently, once the signature (rights manager certificate) from a component is loaded into the operating system, the component can be subsequently removed from the computer and later reconnected without any effect on the determination of trustworthiness of that component by the operating system (Blocks 303-309).

For at least this reason, England does not disclose at least "concluding within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion thereof" of Claim 60 or the corresponding recitations of the other independent claims. Moreover, as Applicants explained in the Amendment filed on October 26, 2004, neither Bjorn nor Matchett teach or suggest this recitation.

Consequently, Applicants respectfully submit that the pending claims are patentable over Bjorn in view of Matchett for at least the reasons that were explained in their earlier Amendment dated October 26, 2004, and further submit that the pending claims are also patentable over a further combination of Bjorn and Matchett in view of England for at least the reasons explained above.

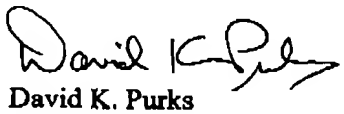
Applicants Previously Filed Terminal Disclaimer Overcame the Still-Pending Provisional Obviousness-Type Double Patenting Rejection:

Applicants note that the Final Office Action appears to continue to reject the pending claims based on the nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,844. Applicants previously filed a Terminal Disclaimer on October 26, 2004, concurrently with the Amendment filed on that date, which disclaimed additional term over the copending U.S. Application Serial No. 09/764,844. Accordingly, withdrawal of the obviousness-type double patenting rejection is respectfully requested.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

Respectfully submitted,



David K. Purks
Registration No. 40,133

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401